High-Profile COMPLIANCE

The compliance function has come a long way from checking boxes.

By **M Siva Shankar** (left), Consultant,
and **G Sudhir** (right), Associate Consultant

What happens if the recent spate of very costly financial settlements by banks becomes a routine occurrence rather than temporary setbacks? In that case, the threat of punitive penalties would spur a compliance race among the top banks.

Now that major banks have agreed to pay record-setting fines and penalties for various compliance lapses, it may prove difficult for budget-challenged governments to turn off the spigot on such a rich potential source of revenue. If that scenario manifests itself, it won't be good enough just to satisfy a static set of requirements. Instead, banks will have to outperform their competitors at compliance lest they become subject to additional regulatory scrutiny for not keeping up. In turn, financial institutions will have a strong incentive to build best-in-class compliance capabilities.

No matter how the relationship evolves between regulators and the financial services industry, the clear message is that compliance has become a board-level and executive-level concern. Instead of compliance being considered as a support function – a cost center responsible for ticking the right boxes – the emerging view is that compliance has become a profit center that should aim to protect other sources of revenue from fines and penalties.

Through the strategic allocation of IT and human resources, financial institutions can achieve a sustainable competitive advantage by gaining a reputation for compliance excellence in key lines of business. Given the increasing compliance risk, mediocre compliance organizations will operate at an ever-growing disadvantage to institutions with a stronger compliance focus. Accordingly, if an executive team intends to dominate a particular line of business, compliance has to be considered a core competency. The compliance dimension can make or break long-term strategies involving decisions of which geographies to enter, which types of clients to serve and at what price points and even which products to offer in the marketplace.

Even as the expectations ratchet up on financial institutions, new technology is making it harder to become a best-in-class compliance organization. The economy has globalized and new payment instruments have followed with expanded options for mobile, person-to-person and business-to-business payments. In this regard, legacy techniques are no longer sufficient – or sufficiently scalable – to address two of the major concerns of governments: Money Laundering (ML) and Terrorist Financing (TF).

The combination of increased scrutiny and increased difficulty has led financial institutions' top executives to investigate new approaches to software, strategic sourcing and various organizational constructs. The new compliance organization has to be **faster** to keep up with higher payment volumes, **smarter** to keep up with growing regulatory complexity, and more **flexible** in order to incorporate new payment methods into existing processes.

TCS BaNCS **COMPLIANCE**

TCS BaNCS offers a comprehensive compliance solution with end-to-end capabilities covering the fundamental regulatory requirements of banks and financial institutions. The solution supports AML, anti-terrorist financing and KYC regulations using both real-time and batch monitoring workflows, and offers a complete range of regulatory reports for multi-entity, multi-jurisdictional firms.

TCS BaNCS provides a solution compliant with Financial Action Task Force (FATF) requirements and other regulatory demands across the financial enterprise, through its business modules for KYC, Watch List Scanning, Transaction Monitoring, Case and Alert Management, Workflow and Reporting.

Also, in response to high levels of customer demand, TCS BaNCS provides a rapid readiness solution for FATCA compliance, including Customer Profiling and Reporting. TCS also provides know-how to financial institutions in making necessary changes to handle requests for withholding tax.

Depending on market needs, deployment models for TCS BaNCS can be standalone implementations; hosted hardware for AML applications; and fully hosted, integrated solutions.

As part of the product roadmap, in September 2014, TCS released a major update (version 7) of TCS BaNCS for Compliance. The update makes the underlying data model of the application more flexible in meeting financial Institutions' growing reporting needs. The update also improves performance of watch-list scanning and provides enhanced capabilities for capturing a 360-degree view of customers across the enterprise.

ISTOCKPHOTO

FASTER COMPLIANCE

Anti-money laundering (AML) and Know-Your-Customer (KYC) programs have driven steady growth in IT budgets. While automated solutions are excellent at finding possible discrepancies and generating alerts, they have not kept pace with the increasing volume of payments, higher complexity of global transactions or faster velocity of payments. Even if a suspicious transaction is detected, there is only a small window of opportunity for the right someone to act. Even if an automated solution excels at uncovering suspicious transactions, it still takes human oversight to turn an alert into an effective – that is, an appropriate – response.

In the initial days of AML awareness, people were the first line of defense in the fight against money laundering. Today, sophisticated AML systems have become the first line of defense – with people and procedures necessary for much-needed backup.

Nevertheless, financial institutions are still reluctant to bolster the automated solutions with an adequate support structure, either using full-time employees (FTEs) or business process outsourcing (BPO).

For payment methods considered highly critical for a bank's strategy -- or for those methods highly vulnerable to exploitation – the need of the hour is "on-line, real-time" monitoring. The goal should be to detect and prevent ML and TF at their point of origination, which can only occur through a solution that combines automation with well-trained human oversight.

The right number of FTEs and the appropriate level of BPO engagement depend upon the characteristics of the financial institution: geographies, customers, products and services, and firm-specific vulnerabilities. Within that framework, each organization has to define how to support straight-through processing for the underlying business while also quickly and accurately resolving situations that may indicate potential abuse of the banking system.

An AML solution – including IT solutions, people and processes – must handle a large volume of transactions while assessing an appropriate level of scrutiny on each individual transaction. Too many "false negatives" opens up the bank to regulatory risk, while too many "false positives" creates an unnecessary or even unsustainable oversight burden. It's a moving target, as the right balance between speed and scrutiny changes morphs under both business and regulatory pressures.

SMARTER COMPLIANCE

The total compliance solution also has to provide, for each regulatory jurisdiction in which a financial institution does business, heightened levels of detail about customer accounts and transactions.

The immediate challenge for financial institutions is the U.S. Foreign Account Tax Compliance Act, or FATCA, a far-reaching regulation that started to take effect in July 2014 requiring banks around the world to report to the U.S. any relevant information about accounts held by U.S. persons including corporate entities.

As a first step to meeting the requirements of FATCA, financial institutions have to conduct due diligence across their existing customer base to identify U.S. persons and establish a set of new processes for monitoring and reporting account details and transactions directly to the U.S. tax authorities. In countries that participate through an Intergovernmental Agreement (IGA), financial institutions will be able to report to their own governments, which will in turn consolidate and share information with the U.S. Furthermore, if a bank fails to provide the requested information about a customer, its U.S. counterparties will be forced to apply a 30 percent withholding tax to related transactions. The complex interactions of these requirements make the FATCA compliance effort a monumental one.

The European Union is the source of another impending set of proposals published in May 2013: the fourth E.U. Anti-Money Laundering Directive along with an updated regulation that calls for "due traceability" of information accompanying transfers of funds. Both of these proposals advocate a risk-based set of guiding principles that extend the responsibilities of financial institutions with regard to anti-money laundering, customer due diligence, politically exposed persons and tax crimes.

One of the main challenges with FATCA and similar regulations is that they involve systems and processes outside of the traditional, bolt-on compliance function. In addition to implementing software for managing specific cases, alerts, workflows and reports, financial institutions also have to give compliance professionals the organizational access and authority to find the information they need to ensure that regulatory concerns are being met at all stages of a transaction. Another important aspect is to assess and enrich the knowledge and capabilities of compliance personnel.

FLEXIBLE COMPLIANCE

As financial services become more integrated into both electronic and offline commerce, various prepaid cards, mobile payments and Internet payment services have gained in popularity as a means of sending funds quickly and efficiently to any connected endpoint.

Unfortunately, these new payment methods, or NPMs, also have potential vulnerabilities in terms of ML and TF. For example, a known terrorist can get a third-party nominee to conduct a transaction, or a money launderer can facilitate payments through an employee or owner of a complicit NPM provider. Through these means, money can be sent outside of the strict constraints of the banking sector, exploiting the lack of face-to-face contact or identity verification to conduct high-speed anonymous fund transfers.

From a compliance standpoint, financial institutions can certainly choose to ignore NPMs, leaving both the compliance challenge and the business opportunity to others. It's an open question as to whether non-bank NPM providers have the breadth and wherewithal to understand and implement the requirements of financial regulations across jurisdictions. However, it does seem likely that non-bank providers will come under intense scrutiny by regulators, especially if specific abuses can be traced to NPMs.

Alternatively, financial institutions can embrace NPMs both in their product lineups and compliance frameworks. Financial institutions can expand their reach into an increasingly digital world either by building their own NPMs or by partnering with NPM providers.

Indeed, some NPM providers have started to partner with established banks to manage their back-end settlement, compliance and reporting requirements. This approach helps both the service provider to ensure that it can operate within the regulations, and the bank in building expertise and experience in NPMs.

Other NPM providers have started to enter into end-to-end agreements with IT-enabled service providers for comprehensive SaaS (Software-as-a-Service) or AaaS (Architecture-as-a-Service) deals. However, this approach is risky in the sense that the service provider may absorb a great deal of responsibility for the cost of non-compliance on behalf of a NPM provider. That contingent liability may be a problem for regulators – as well as for the service provider's other customers.

Consequently, the most likely model for the future development of NPMs will be either a partnership model, where innovative NPM providers rely upon financial institution partners to manage their global compliance and risk management needs; or in some cases, leading banks will themselves take on the role of market innovator by introducing NPMs.

In either case, the winners will be those with the fastest, smartest and most flexible compliance departments. These will be the financial institutions most capable of capitalizing upon the immense profit potential of new payment methods, new business models and new approaches to partnership. ■

RECENT **DEPLOYMENTS**

In the recent quarters, TCS has implemented the Compliance solution of TCS BaNCS at:

- **CTBC Bank (Philippines) Corp.**, the Philippines retail banking subsidiary of Taiwan-based CTBC Bank;
- **First Metro Investment Corporation**, an investment banking, treasury and investment advisory firm based in the Philippines; and
- **Bank of Maharashtra**, one of the largest public-sector banks in India with a focus in retail and corporate banking.

One of the common features across these implementations was the establishment of on-line, real-time "know-your-customer" checks during customer on-boarding. Each of these deployments also supports regulatory reporting requirements with end-to-end audits of their AML and KYC activities to establish who did what and when.

Each of these recent deployments span various business units, giving the compliance teams the ability to build a comprehensive knowledge base while allocating resources efficiently to the areas with the most critical needs.